



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

Address: COMMISSIONER FOR PATENTS

P.O. Box 1450

Alexandria, Virginia 22313-1450

www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

09/923,075

08/06/2001

Lynn Henry Wheeler

34250-1174

1892

7590
Malvern U. Griffin III
SUTHERLAND ASBILL & BRENNAN LLP
999 Peachtree Street, N.E.
Atlanta, GA 30309-3996

07/17/2008

EXAMINER

PYZOCHA, MICHAEL J

ART UNIT

PAPER NUMBER

2137

MAIL DATE

DELIVERY MODE

07/17/2008

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

09/923,075

Applicant(s)

WHEELER ET AL.

Examiner

MICHAEL PYZOSHA

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 23 April 2008.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-39 is/are pending in the application.
- 4a) Of the above claim(s) 1-11 is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 12-39 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
- 4) ☐ Interview Summary (PTO-413)
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

1. Claims 1-39 are pending. Claims 1-11 have been withdrawn from consideration.
2. Amendment filed 04/23/2008 has been received and considered.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 12, 14-17, 21, 23-26, and 30-39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fischer (US 5422953) in view of McClain et al. (US 6049874) and further in view of Yasukura (US 6990588).

As per claims 12, 21, 38 and 39, Fischer discloses a method and system for providing a random number for utilization in a computer program application that requires the random number, the method comprising the steps of: creating a private key of a public/private key pair within a secure device (see figure 2 numeral 24 and column 3 lines 44-46; column 4 lines 29-41; and column 7 lines 56-59); comparing pre-stored verification data to input verification data received from a user of the secure device (see column 7 lines 51-62); upon receipt of message data at the secure device originating a digital signature for the message data, the originating comprising (see column 7 lines 43-50): calculating a hash value for the message data; encrypting the hash value using

the private key (see column 7 lines 51-62); providing the results of the encrypting step as a generated digital signature (see column 7 lines 51-62) providing to the computer program application external to the device the generated digital signature constitutes a random number for use by the computer program application (see 7 lines 63-67).

Fischer fails to explicitly disclose the use of a digital signature as a random number for secure electronic communications and fails to disclose creating a verification status indicator, based on a comparison of verification information that is a component of the digital signature.

However, McClain et al. teaches using a digital signature as a random number for secure electronic communications (see column 12 lines 28-57) and Yasukura teaches including an authentication result (i.e. verification status indicator) with a transaction (see Yasukura column 17 line 66 through column 18 line 2).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the digital signatures of Fischer as a random number for secure electronic communications and for the message to include an authentication result.

Motivation to do so would have been to provide a unique session specific session key for encryption (see McClain et al. column 12 lines 28-29) and so that a second part can determine if a transaction should be accepted or refused (see Yasukura column 17 line 66 through column 18 line 2).

As per claims 14 and 23, the modified Fischer, McClain et al. and Yasukura system discloses using the generated digital signature to generate a session key for secure electronic communications (see McClain et al. column 12 lines 28-57).

As per claims 15 and 24, the modified Fischer, McClain et al. and Yasukura system discloses the digital signature is generated within a computer chip within the device (see figure 1 and column 3 lines 25-38).

As per claims 16 and 25, the modified Fischer, McClain et al. and Yasukura system discloses the computer chip itself includes a random number generator (see figure 1 numeral 10 and column 4 lines 1-15).

As per claims 17 and 26, the modified Fischer, McClain et al. and Yasukura system discloses the digital signature is generated within the computer ship using the private key and a random number obtained from the random number generator (see column 4 lines 1-15).

As per claims 30 and 34, the modified Fischer, McClain et al. and Yasukura system discloses the computer program application is a security protocol (see McClain et al. column 12 lines 28-57).

As per claims 31, 32, 35, and 36, the modified Fischer, McClain et al. and Yasukura system fails to explicitly disclose the security protocol is SSL and PGP.

However, Official Notice is taken that at the time of the invention one of ordinary skill in the art would recognize to use the random numbers of the modified Fischer, McClain et al. and Yasukura system in SSL and PGP. Motivation to do so is that these are two well-known security protocols that use random numbers.

As per claims 33 and 37, the modified Fischer, McClain et al. and Yasukura system discloses the computer program application is a digital signature algorithm for generating a digital signature (see Fischer column 7 lines 51-62).

5. Claims 13 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Fischer, McClain et al. and Yasukura system as applied to claims 12 and 21 above, in view of Binding et al. (US 6775772).

As per claims 13 and 22, the modified Fischer, McClain et al. and Yasukura system fails to disclose the use of the digital signature to distinguish and prevent a replay attack.

However, Binding et al. teaches the use of a digital signature on a nonce to distinguish and prevent a replay attack (see column 9 line 64 through column 10 line 11).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the digital signature as a safeguard against a replay attack.

Motivation to do so would have been to verify the identity of each party in the communication.

6. Claims 18 and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Fischer, McClain et al. and Yasukura system as applied to claims 17 and 26 above, and further in view of Applicant's Admitted Prior Art (hereinafter AAPA).

As per claims 18 and 27, the modified Fischer, McClain et al. and Yasukura system discloses the use of other digital signature algorithms (see Fischer column 3 lines 56-60) but fails to explicitly disclose the use of an elliptical curve digital signature algorithm.

However, AAPA teaches that an elliptical curve digital signature algorithm is a common way to generate a digital signature (see paragraph 146 [page 26 line 32-36]).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use an elliptical curve digital signature algorithm because doing so is a common way of generating a digital signature.

7. Claims 19, 20, 28, and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Fischer, McClain et al. and Yasukura system in view of AAPA as applied to claim 18 and 27 above, and further in view of Wang (US 6594759).

As per claims 19, 20, 28 and 29, the modified Fischer, McClain et al. and Yasukura system in view of AAPA discloses the chip being tamper resistant (see Fischer column 3 lines 31-38), but fails to explicitly disclose the random number generator is inaccessible from outside the computer chip.

However, Wang teaches that the random number generator can be used solely by a computer chip (see column 13 line 49 through column 14 line 6).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to make the random number generator of the modified Fischer, McClain et al., Yasukura and AAPA system be inaccessible from the outside.

Motivation to do so would have been to increase the security of the system.

Response to Arguments

8. Applicant's arguments with respect to claims 12-39 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

9. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL PYZOSKA whose telephone number is (571)272-3875. The examiner can normally be reached on Monday-Thursday, 7:00am - 4:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2137

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MJP

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2137